

PATENT  
Attorney Docket No. 1948/US/2  
USPTO Facsimile No. (703) 872-9306

**Amendments to the Specification:**

Please replace the paragraph beginning at page 1, line 1, (paragraph [0001]) with the following paragraph, marked to show changes:

[0001] This application claims priority to United States Provisional No. 60/452,369, entitled "METHOD AND APPARATUS FOR IDENTIFYING, MANAGING, AND CONTROLLING COMMUNICATIONS," naming John R. Klug as Inventor and filed on March 5, 2003, the entirety of which is hereby incorporated by reference. This application is also related to co-pending application serial no. ~~xxxxxx~~ 10/673,017 (Attorney Docket No. 1948/US/3), also entitled "METHOD AND APPARATUS FOR IDENTIFYING, MANAGING, AND CONTROLLING COMMUNICATIONS," naming John R. Klug as inventor and filed on September 27, 2003, the entirety of which is also incorporated herein by reference.

Please replace the paragraph beginning at page 2, line 1, (paragraph [0005]) with the following paragraph, marked to show changes:

[0005] Commonly today, users of computing and/or telecommunications devices often receive untold numbers of communications from various persons, entities and/or automated systems. Many of such communications are unwanted and are often considered undesirable by recipients and others for various reasons. In addition, users of commercially provided, corporate provided and/or individually provided electronic mail ("e-mail") accounts receive dozens, or even hundreds, of unwanted e-mail communications daily. Regardless of whether an e-mail account is provided by ~~MICROSOFT~~ Microsoft (e.g. via their MSN and/or HOTMAIL services), ~~[YAHOO]~~ Yahoo (e.g. via its web-based e-mail services), or via various corporate e-mail services and/or applications (for example, via a Microsoft Exchange Server connected to a desktop and/or other computing device on which an e-mail application, such as ~~MICROSOFT~~ Microsoft OUTLOOK, and/or other desktop applications may be running), e-mail communication users (and user of other forms of communications) are subjected daily to numerous unwanted e-mails/communications. These unwanted e-mails/communications are often commercial solicitations in which the recipient has little if any interest, and are commonly referred to as "spam," "mass e-mails," or the like. Today, spam makes up a significant percentage of all e-mail traffic. The amount of spam e-mail users receive today has led many users to simply stop using e-mail as a communications medium.

PATENT  
Attorney Docket No. 1948/US/2  
USPTO Facsimile No. (703) 872-9306

Please replace the paragraph beginning at page 15, line 15, (paragraph [00046]) with the following paragraph, marked to show changes:

[0046] Upon receipt of the franked e-mail/communication, 105 the recipient system 125 may analyze the frank 110 and sort the communication accordingly. For example, the recipient system 125 may be an IBM/PC compatible computer which has an e-mail/communication application 130 resident thereon, such as OUTLOOK, manufactured by ~~MICROSOFT~~ Microsoft Corporation of Redmond, Washington, or EUDORA Eudora Mail, manufactured by QUALCOMM Qualcomm Incorporated, of San Diego, California, or INSTANT MESSENGER, manufactured by ~~AMERICA-ONLINE~~ America Online Corporation. The communication program 130 may also be a separate program (or portion of a larger program) configured to receive, acknowledge, and/or process a frank 110 or franked communication 105. Alternately, the recipient system 125 may be any form of device of computer described herein.

Please replace the paragraph beginning at page 17, line 6, (paragraph [00050]) with the following paragraph, marked to show changes:

[00050] It is to be appreciated that in mail-exchange server topologies, a recipient's system 125 or device (such as a personal computer) may include e-mail/communication software 130 that is configured to perform ranking and presentation, as appropriate, of franked communications 105. Similarly, in embodiments wherein a mail-exchange server is not utilized or communications are not received via a local software application 130 and instead are received via a network or server based application (for example, from a communications feature provided by an ISP server or a remote computing application, such as that supported by Citrix Systems and other like systems), the filtering and ranking may occur at the service provider's (and/or a third party's) server or system instead of the recipient's system 125. The results of such filtering and ranking may be provided via HTML pages, XML pages, Flash implementations, Java implementations and/or any other types of information transfer formats supported by a given service provider and compatible with a recipient's given device(s). Commonly, but not necessarily, such information transfer may occur via Web browser compatible information formats, such as those supported by Microsoft ~~Internet Explorer~~ INTERNET EXPLORER, Netscape Navigator NAVIGATOR and others.

PATENT  
Attorney Docket No. 1948/US/2  
USPTO Facsimile No. (703) 872-9306

Please replace the paragraph beginning at page 24, line 17, (paragraph [00067]) with the following paragraph, marked to show changes:

[00067] Another approach for reducing and/or eliminating undesired communications 105, such as spam, utilizes recipient permissions and approved sender lists. In general, a permission-based software application (not shown), such as that provided by Choice Mail ~~CHOICE MAIL~~, may be loaded onto a recipient device 125 or utilized at an ISP 225 associated with a given recipient device 125. In this approach, the application generally does not try to identify and block spam (see, for example, the Wall Street Journal article "Choice Mail Designs Best Traffic Cop Yet to Thwart Spammers," July 11, 2002, incorporated herein by reference). Instead, the application determines whether a given sender has the recipient's permission to send the recipient an e-mail/communication 105. Upon belief, the ~~CHOICE MAIL~~ Choice Mail system and similar approaches may utilize a look-up table containing a list of approved senders. The look-up table may be stored on the recipient's device 125 or at a network node 135. Accordingly, whenever an e-mail/communication 105 from an unapproved sender is received, permission is requested or verified from the recipient prior to the e-mail/communication entering the recipient's e-mail/communication inbox.

Please replace the paragraph beginning at page 26, line 8, (paragraph [00070]) with the following paragraph, marked to show changes:

[00070] However, it is to be appreciated that certain embodiments of the present invention may utilize a franking system wherein unfranked e-mails/communications 105 are automatically discarded. In such an embodiment, it is foreseeable that an unfranked e-mail/communication 105 from a sender on a given recipient's approved sender list 235 might be discarded before reaching the recipient's ISP 225 and/or presentation device/system 125. As such, various embodiments of the present invention may also be configured such that approved sender lists 235 are communicated to clearing house servers (not shown). As used herein, "clearing house servers" generally remove an unfranked e-mail/communication 105 from a given network 120 unless the e-mail/communication is from an approved sender, as identified by a recipient's approved sender list 235. Currently, it is believed that most U.S. domestic Internet traffic passes through a handful of central servers. Such central servers may be configured to act as such clearing house servers. Similarly, large ISPs 215, 225 (such as ~~AMERICA ONLINE~~ America Online, MSN, ~~[YAHOO]~~ Yahoo, and others) might also be suitably configured as clearing house servers.

PATENT  
Attorney Docket No. 1948/US/2  
USPTO Facsimile No. (703) 872-9306

Please replace the paragraph beginning at page 28, line 7, (paragraph [00075]) with the following paragraph, marked to show changes:

[00075] Generally, in the present embodiment a sender may establish an electronic credit or debit account 310 with either the operator of the franking server 305 or a third party prepared to act as a payment intermediary between the sender and the franking server operator (for example, those provided by PayPal PAYPAL, Western Union and the like). These credit and debit accounts 310 may correspond to any association of "value" specified by the parties. Examples of such "value" may include monetary value (e.g., United States dollars), points or credits (such as frequent flyer miles), credit or a promise to pay at a later date, or any other negotiable, mutually acceptable items or measures. Similarly, the term "payment" as used herein generally refers to any such exchange of a mutually valued or accepted item. A sender (for example, a mass e-mailer or telemarketer) may use the account 310 to purchase or obtain franks 110 from the franking server 305. These franks 110 may be attached to, associated with, or incorporated into an e-mail/communication 105 or communication for transmission to a receiver.

Please replace the paragraph beginning at page 44, line 18, (paragraph [000113]) with the following paragraph, marked to show changes:

[00113] Fig. 7 displays a second version of a franking application 700, wherein the franking application 700 interfaces with a web browser 705 (such as, for example, those provided by Microsoft INTERNET EXPLORER or NETSCAPE Netscape). Here, the franking application 700 may again take the form of an API or application in communication with the browser 705. However, it may also be configured as a browser plug-in, JAVA script, ActiveX script, XHTML script, XML script, SGML script, VB script, HTML script or other such scripting language or protocol. Further, the franking application 700 may be remote to the sender's system 115 and accessible by the browser 705 through a network 120, and not resident on the sender's system at all. Thus, the franking application 700 may be a purely ASP-based solution which may be, for example, co-hosted with the franking server 305.

Please replace the paragraph beginning at page 69, line 13, (paragraph [000184]) with the following paragraph, marked to show changes:

[000184] Generally, senders pay for franks 110 on a per frank basis from either a credit or a debit electronic account. The franking server 305, 900, 905, 910 may withdraw

PATENT  
Attorney Docket No. 1948/US/2  
USPTO Facsimile No. (703) 872-9306

funds directly from a sender's bank account, for example, provided that the sender authorizes such electronic withdrawal. Alternately, the sender may specify a credit card, a ~~PAYPAL~~ PayPal account, or other conventional third party electronic debit account for use with the franking system. In an alternate embodiment, the sender may establish a credit or debit account 310 directly with the franking system itself or an entity in fiscal partnership with the franking server.

Please replace the paragraph beginning at page 77, line 1, (paragraph [000203]) with the following paragraph, marked to show changes:

[000203] Generally speaking, the above embodiments have been described in the context of a sending 115 and receiving 125 e-mail/communication server. Such servers rely on both the sender's and recipient's systems running an e-mail/communication application program 600, 700, 805. However, in many cases, either senders or recipients are limited in their e-mail/communication 105 access. For example, many corporations place firewalls around corporate e-mail/communication servers 615, 225 in order to limit electronic mail access by their employees. Accordingly, the present invention also contemplates a Web based embodiment. A sender or recipient may access a dedicated Web site which enables them not only to send or receive electronic mail (such as web sites provided by Microsoft's HOTMAIL or [YAHOO] Yahoo MAIL) and/or other forms of communications but also has inherent franking functionality. A sender may efficiently and easily frank any and all e-mails/communications 105 sent from such a Web based embodiment. Similarly, a recipient accessing this embodiment may be assured that, unlike an e-mail/communication application 130 resident behind a firewall, the Web based server will properly filter and categorize all franked communications 105.